RESULTS OF THE CANDU 3 PROBABILISTIC SAFETY ASSESSMENT

R.K. Jaitly

AECL CANDU
446A, 2nd Ave. North
Saskatoon, Saskatchewan
Canada S7K 2C3

Introduction

The CANDU 3 is one of the next generation models of the CANDU reactors. It provides the economy of operation of other CANDUs in a smaller unit size (450 MW). The design makes use of proven technology from the larger CANDU units along with updated relevant features from ongoing Canadian research and development. A key part of the CANDU 3 design program is a review of the design by the Canadian regulatory (AECB) prior to the start of construction. These up front licensing discussions provide an opportunity for the AECB and industry to explore and resolve the main issues during the design stage. Including Probabilistic Safety Assessment (PSA) as part of the design process was seen as one valuable way of ensuring that safety related requirements are defined early. These measures minimize the probability of engineering rework during and after plant construction. In addition the PSA is being used in the traditional role in safety assessment and licensing. This paper provides a summary of the CANDU 3 PSA work and the results thereof.

CANDU 3 PSA Program

The purpose of the CANDU 3 PSA was:

i. to provide safety design assistance in the early stages of design to ensure that the design includes adequate redundancy and functional separation of mitigating systems,

ii. to identify accident sequences that could be large contributors to public risk,

iii. to calculate the summed core damage frequency for the CANDU 3 design

iv. to identify operator actions required to mitigate the consequences of accidents and thus provide an input to emergency operating procedures,

v. to provide input to the environmental qualification program and control centre design, and

vi. to provide an input to the test and maintenance programs such that they can be optimized in terms of cost and safety.

It was decided to tackle the PSA program in four distinct phases viz: Mini PSA, Conceptual PSA , Generic PSA and the Site Specific PSA. The Mini PSA phase consisted of a review of the proposed CANDU 3 design concept for three initiating events, that the past CANDU PSAs had shown were the main contributors to core melt frequency viz: loss of service water, loss of off–site power and a small LOCA. As a result of this work a number of design improvements were identified and incorporated in the design. The Conceptual PSA phase involved a review of the design for a much wider selection of events. These events were identified from a systematic review of the conceptual design, CANDU operating experience and the AECB's consultative document C–6. A total of 84 events for the plant operating and the shutdown state were addressed in the Conceptual PSA. One of the primary objectives of this PSA was to establish reliability targets based on past PSA studies, engineering judgement and / or simple fault tree analysis. This was seen as a valuable input to the early design process when most design changes can be implemented at a minimal cost.

The Conceptual PSA work is now complete and the results are presented in this paper. The Generic PSA will be a detailed PSA for the Standard CANDU 3 design. It will consist of verification of the system reliability targets established by the Conceptual PSA. The verification will be carried out by

rigourous fault tree analysis for the detailed design and where cross–links exist, the fault trees will be merged to give a more accurate assessment of the plant performance. Thus the Generic PSA will be done to state–of–the–art standards and methodology. The Generic PSA will also include a Level II PSA to assess containment performance for the purpose of identification of the source terms at the containment boundary. This will be accomplished by the development of a containment event tree. This tree will use common event tree construction methods, and will pose questions regarding the success/failure of various containment sub–systems. Typical containment failure modes to be considered are:

- total loss of air coolers (includes failure of H_2 control, dispersion, ignition), and
- failure of containment isolation.

For the cases where the plant that is constructed deviates significantly from the generic design because of customer request or local siting or licensing requirements, a site specific PSA will be carried out.

PSA Based Engineering Insights and Design Decisions

The thrust of the Conceptual PSA (CPSA) for CANDU 3 was to provide safety assistance in the early stages of design to ensure that the design includes adequate redundancy and functional separation of the mitigating systems. Based on acceptance criteria for limiting public releases, a desired level of safety was first established for CANDU 3. This is defined in terms of limiting a) the frequency of the individual event sequences with no heat sink to less than 10^{-6}/year and b) the frequency of the individual event sequences requiring moderator as heat sink to less than 10^{-4}/yr. With this objective in mind, a Level I PSA by event tree analysis was performed. The event tree analysis work enabled the reliability and performance requirements for the safety related systems to be set. These were documented in an overall plant performance specification. This specification also defines the system interface requirements with respect to control and electrical power, instrument air and service water. The system designers are applying this in the development of the detailed CANDU 3 design.

The performance of CPSA for CANDU 3 led to a variety of engineering insights and helped in finalizing a number of design decisions. These are summarized below:

Engineering Insights

i. Input to Control Room Design

The CPSA identified need for corrective operator actions in response to the initiating events. As a result, the required alarms and annunciations were identified to enable the operator to perform the actions. The PSA team is also in the process of preparing operator response guidelines (ORGs) to be later used in the preparation of emergency operating procedures (EOPs) by the utility. The ORGs are being prepared to provide assistance in the control centre design by identifying alarms and annunciations needed by the operator for mitigating consequences of the major abnormal events. For all accident conditions, the operator must be able to monitor the major process parameters,

for example:
- reactor power,
- Heat Transport System pressure,
- Heat Transport System temperature,
- Steam Generator pressure,
- Steam Generator level,
- containment pressure.

ii. Operator Action Time for Corrective Actions

One of the design intentions of CANDU 3 was to minimize the need for corrective operator actions following an accident. The CPSA work has demonstrated that for most of the accidents, operator actions are not needed for nearly 8 hours as long as the front line mitigating systems are functional. This is

achieved primarily by the feature of the Group 2 feedwater system. This system is automatically initiated and has capacity for decay heat removal for approximately 10 hours. There are a few exceptions i.e. for a small number of events, operator actions is required sooner than 8 hours to prevent fuel damage. These are:

- Feedwater (or boiler blowdown) line breaks between the steam generator and the check valve: This will render the Group 2 feedwater supply to be lost via the break. Operator action will be required in approximately 30 minutes to isolate the affected boiler or initiate Shut Down Cooling.
- Steam generator tube rupture: This will lead to Heat Transport System depressurization requiring Emergency Core Cooling to fire. Once Emergency Core Cooling fires, the Emergency Core Cooling System inventory will be lost via the ruptured tube and the main steam safety valves. Operator action is required within 90 minutes to meet the dose limits for Class 1 of Reference 4, assuming conservative methodology. (The Emergency Core Cooling System inventory will be exhausted in about 24 hours without operator action).
- A small LOCA (say a feeder break) during the plant shutdown state (Heat Transport System cold and depressurized) requiring operator to manually initiate Emergency Core Cooling in approximately 30 minutes to prevent fuel overheating.
- Loss of Shut Down Cooling heat sink during the plant shutdown state when Heat Transport System is drained to the header level: Within 1.5 hours, this condition will require operator actions to supply Group 2 Raw Service Water to the Shut Down Cooling heat exchanger (for loss of Group 1 Recirculated Cooling Water), or bottle–up and fill–up the Heat Transport System to enable the use of boilers as heat sink (for loss of Shut Down Cooling pumps).

iii. Input to Plant Layout Design Reviews

In analyzing steam line and feedwater line breaks in various locations of the plant, the need for certain equipment to be immune from the steam environment was identified. Such equipment (for example; service water pumps, electrical power distribution system) was then included in the environmental qualification program, or relocated to protected area.

iv. Input to Maintenance and Testing

As part of the PSA process, test intervals, and maintenance restrictions are defined. A number of maintenance considerations for the plant shutdown state were identified by the CPSA. For example:

- Rapid bolt up and fill up provisions for the Heat Transport System to allow steam generators to function as a heat sink in the event of problems with the Shut Down Cooling heat sink when the Heat Transport System is drained to the header level.
- Restrictions on the number of boiler feed water pumps and on site diesels which can be taken out for maintenance at a time.

v. Improved Independence Between Process Systems

During the early stages of CPSA work, there was a concern that the assumed independence among initiating events and the credited mitigating systems might be invalidated if the plant systems were to share Distributed Control System equipment such as control processor modules, input/output modules and communication highways. As a result, an assessment was done to provide confidence that the Distributed Control System system can be designed and configured to meet process function independence requirements. This assessment led to a number of insights regarding the Distributed Control System design and which operator actions need to be independent of alarms by the Distributed Control System.

Design Decisions

The CANDU 3 event tree analysis work helped in finalizing a number of design changes. These are summarized below:

i. Improved Service Water Reliability;

- Four Raw Service Water pumps and minimum use of expansion joints in the Raw Service Water System,
- Raw Service Water System to have two trains,
- Rubber expansion joints in the Recalculated Cooling Water System to be replaced with victaulic couplings,
- Testable check valves in the Recirculated Cooling Water and the Raw Service Water Systems, and
- Approximately 30 L/s (400 IGPM) make-up to Group 1 Recirculated Cooling Water.

ii. Improved Emergency Core Cooling Reliability;
- Reduction in number of valves,
- Auto change–over to recirculation phase,
- Sustained low flow conditioning, and
- Two Heat Exchangers.

iii. Two redundant groups of service water supply to the shutdown cooler (Group 1 Recirculated Cooling Water and Group 2 Raw Service Water) for improved shutdown cooling capability.

iv. Auto HT Pump Trip on High Bearing Temperature;
- Prevents potential seal failure and small LOCA, and
- Safeguards against lubricating oil fire.

v. Light water make-Up to Heat Transport System to enable handling of small LOCAs without invoking Emergency Core Cooling.

vi. Improved feedwater reliability via two independent sources of high pressure auxiliary feedwater - one of them Design Basis Earthquake qualified, the other utilizing an auxiliary diesel driven pump to cope with station blackout conditions.

vii. Reactor power set back to 2% in the event of low Shield Tank level or low Shield Cooling flow.

viii. Reduction in the number of pneumatic valves to minimizes effects of loss of instrument air.

ix. Four onsite power diesel generators resulting in reduction in station blackout frequency by an order of magnitude (compared with CANDU 6) to 1.29×10^{-5}/yr. Together with the provision of a diesel driven auxiliary feedwater pump, this provides ample time for recovery by the operator.

x. Moderator make-up capability from the Reactor Building floor resulting in reduction of core damage frequency following a feeder stagnation break and loss of Emergency Core Cooling to less than 10^{-6}/yr.

xi. Steam Generator blowdown isolation valve auto closure in the event of a pipe break to preserve feedwater inventory.

CANDU 3 PSA Results

The main results of the Conceptual PSA relating to failure to shutdown and core damage frequencies are summarized below:

Failure to Shutdown Frequency

The summed frequency of failure to shutdown for all initiating events is 1.9×10^{-8}/yr. This is a conservative number since the event trees used a failure to trip probability of 10^{-3} for each of the two shutdown systems. This probability is based on the minimum licensing requirements. CANDU operating experience indicates that these two systems have failure probabilities substantially less than 10^{-3}. Furthermore, it was assumed that all initiating events requiring a shutdown, need full design capabilities of the shutdown systems. In reality, for a large number of events the reactor shutdown can be achieved with partial capability of the trip systems.

Summary of Core Damage Frequencies

As required by the PSA acceptance criteria, individual event sequences related to severe core damage, have a frequency less than 10^{-6} events per year. Individual event sequences where moderator is acting as the heat sink have a frequency of less than 10^{-4} events per year. The summed core damage frequency for CANDU 3 is follows:

a. Plant Operating State

The summed core damage frequency for the plant operating state is 5.78×10^{-6}/yr. The dominant contributors to core damage are:

- Feeder break followed by failure of Group 1 Recirculated Cooling Water and failure of the Emergency Core Cooling heat exchanger valves, which permits flow from Group 2 Raw Service Water (3.51×10^{-7}/yr),
- End Fitting break followed by failure of Group 1 Recirculated Cooling Water and failure of the Emergency Core Cooling heat exchanger valves, which permits flow from Group 2 Raw Service Water (3.51×10^{-7}/yr),
- Loss of Group 1 Recirculated Cooling Water and a failure of the bleed condenser to bottle-up when a Liquid Relief Valve sticks open. Subsequently, either the operator fails to take corrective action or Group 2 Raw Service Water is unavailable (2.57×10^{-7}/yr for each case),
- Very small LOCA with a consequential loss of Class IV power followed by unavailability of all Class III onsite standby diesels (1.37×10^{-7}/yr), and
- Loss of shield cooling heat sink followed by failure of the Reactor Regulating System to setback the reactor and failure of the operator to shut down the reactor (1×10^{-7}/yr).

b. Plant Shutdown State

The summed core damage frequency for the plant shutdown state is 2.02×10^{-6}/yr. The dominant contributors to core damage are:

- Loss of Class IV power to all 6.9kV buses (when Heat Transport System is drained to header level) followed by failure of both Group 1 Class III buses to energize and operator failure to take corrective action (4.24×10^{-7}/yr),
- Loss of Class IV power to all 6.9kV buses (Heat Transport System full and depressurized) followed by unavailability of all on site Class III diesels and failure of the auxiliary diesel driven feedwater pump (3.84×10^{-7}/yr), and
- Loss of Group 1 Recirculated Cooling Water when the Heat Transport System is drained to the header level and failure of the operator to take corrective action (2.49×10^{-7}/yr).

Impact of Subsequent Design Changes on Core Damage Frequency

The summed core damage frequency for the plant operating and shutdown state is 7.8×10^{-6}/yr. A breakdown of this frequency is shown in Figure 1. Subsequent to the Conceptual PSA work, a number of design changes were incorporated. In general these design changes will further reduce the CANDU 3 summed core damage frequency as they are related to improvement in the reliability of the mitigating systems, or incorporate additional mitigating systems. Examples of such changes are reduction in Emergency Core Cooling recovery mission time from 6 to 4 months, additional heat transport crash cool–down signal, provision of seismically qualified support services to the shutdown cooling system and moderator inventory make–up.

Conclusions

The thrust of the Conceptual PSA for CANDU 3 was to provide safety assistance in the early stages of design to ensure that the design includes adequate redundancy and functional separation of the mitigating systems. The event tree analysis work enabled the reliability and performance requirements for the

safety related systems to be set. These were documented in an overall plant performance specification. This specification also defines the system interface requirements with respect to control and electrical power, instrument air and service water. The system designers are applying this in the development of the detailed CANDU 3 design.

The performance of this PSA facilitated in finalizing certain design decisions. These include – addition of an independent, seismically qualified Group 2 feedwater system which automatically feeds the boilers at full system pressure in the event of a loss of the Group 1 feedwater system, – improvement to the service water reliability, – setback on loss of shield cooling flow to allow automatic reactor shutdown, – recovery of moderator inventory to mitigate the consequences of a feeder stagnation break with coincident failure of Emergency Core Cooling and – light water make–up to the primary system to handle very small LOCAs without invoking Emergency Core Cooling.

The main results of the Level 1 PSA are:

CANDU 3 Core Damage Frequencies	
From Plant Operating State	From Plant Shutdown State
5.78×10^{-6}/yr	2.02×10^{-6}/yr
Total CANDU 3 core Damage Frequency $= 7.8 \times 10^{-6}$/yr	
Total CANDU 3 Failure to Shutdown Frequency $= 1.9 \times 10^{-8}$/yr	

Acknowledgements

The author wishes to acknowledge the valuable contribution of P. J. Allen and H. S. Shapiro to the CANDU 3 PSA program.

References

1. P. J. Allen, "The Use of PSA in the Design, Safety Assessment and Licensing of the Advanced CANDU Design", PSA 89, April, 1989, Pittsburgh.
2. R. K. Jaitly, P. J. Allen, H. S. Shapiro, J. R. Fisher, S. Naman, "CANDU 3 Conceptual Probabilistic Safety Assessment – Insights and Design Decisions", PSA 91, February 1991, Beverly Hills.
3. P. J. Allen, R. K. Jaitly, "Current Framework For Safety Evaluation In Canada", Technical Committee Meeting on Review of Safety Features of New Designs, November 1991, Vienna.
4. J. R. Fisher, P. J. Allen, S. V. Inamdar, S. Naman, H. Shapiro, "Conceptual Probabilistic Safety Assessment for CANDU 3" , CNS 10th Annual Conference, June 1989, Ottawa .

CANDU 3 CORE DAMAGE CONTRIBUTORS
TOTAL FREQUENCY = 7.8 X 10^{-6} / YR

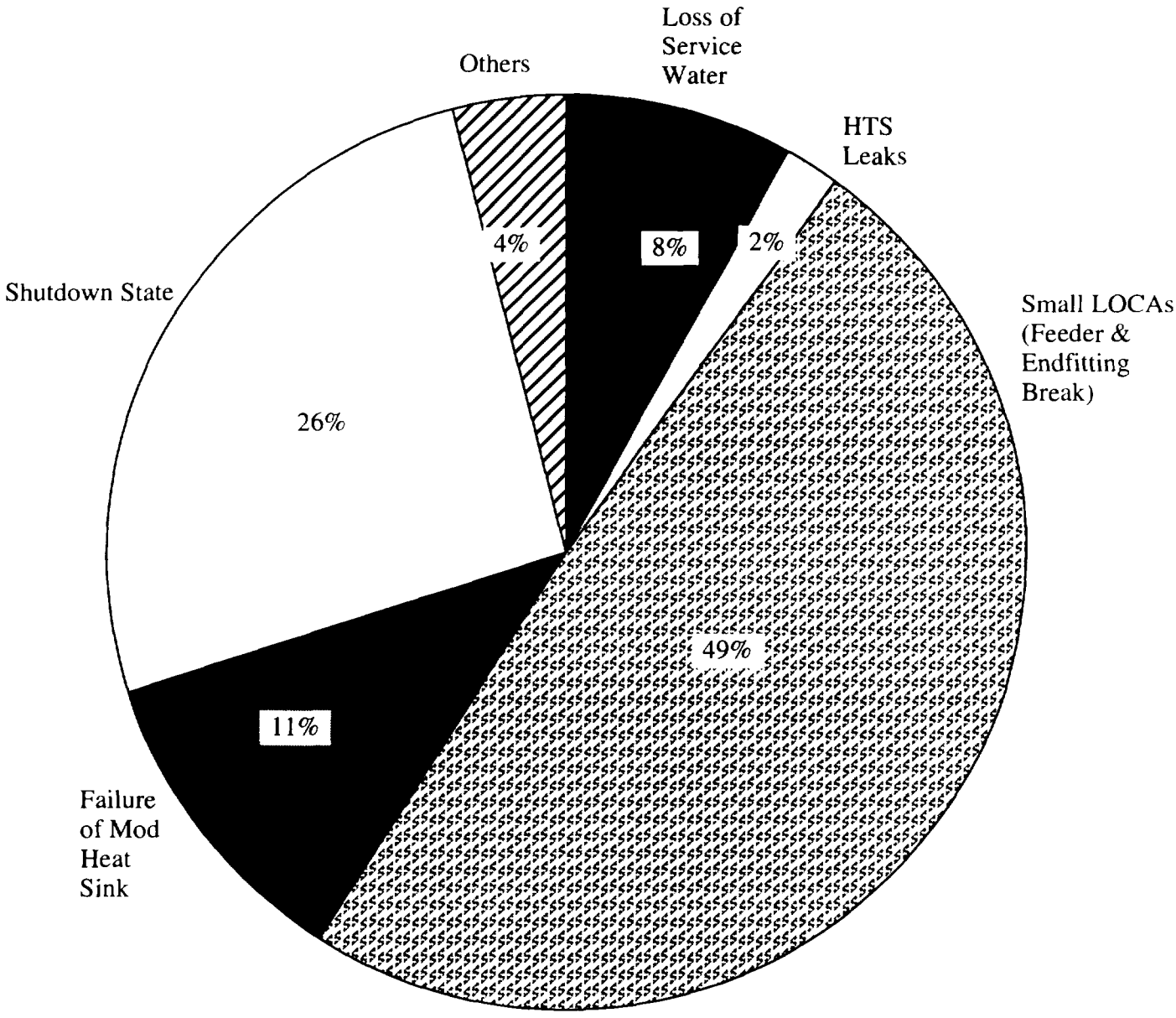

Figure 1: CANDU 3 Core Damage Frequency